DOES SMART HOME HAVE WIDE OPEN DOORS? MQTT COMMUNICATION PROTOCOL STANDARDIZATION - POTENTIAL MISSING RING OF THE IOT NETWORKS SECURITY CHAIN

Ivan Šćepanović[1*], Vesna Šćepanović[1]

[1]Faculty of Management, Sremski Karlovci, University UNION Nikola Tesla, Belgrade;
e-mail: anavesnaivan@gmail.com;

Abstract: This paper pointed out the benefits as well as the security risk that is the result of inconsistencies of software applications from different manufacturers and the lack of standards in IoT devices networks. Message Queue Telemetry Transport (MQTT) is now one of the most used open protocols in the Internet of Things. The term IoT is often followed by a great enthusiasm of researchers. End-users also share the same sentiment, ignoring the security risks that arise from dropping and reconnecting IoT devices that very often send passwords to server in plain text, while manufacturers often remain silently indifferent. They primary put focus on profitability, but not on safety. In other words, the door on smart homes remains wide open for hackers. This paper gives an overview of one potential solution of the Internet of Things security problem.

Keywords: *Internet of Things, MQTT Communication Protocol, Security Risks, Standardization.*

LOOK TO THE FUTURE OF IOT AND BEYOND

Web 3.0 is projected to become a new internet paradigm, an extension and extension for Web 2.0. To this day, there is still a lot of debate about the existence of Web 3.0. Many claim that we have already entered this era, while others disagree and argue that there is still a long way to go.

Web 3.0 is based on the following basis:

- Portability and ubiquity (anywhere, anytime, every device will be connected to the network, meaning content will be available everywhere)
- Personal (focused on the individual, as opposed to the community)
- Dynamic and contextual content
- Artificial intelligence (focuses on natural language processing that computers will understand better than human language and thus ensure that relevant results are obtained faster)
- 3D graphics (three-dimensional design will be used on websites to provide users with a clear picture of products and services)

The semantic web and artificial intelligence are the two cornerstones of web 3.0. Their synergy creates web knowledge characterized by defined meaning, meaning generation, sharing and linking content through search and analysis. Thanks to semantic metadata, Web 3.0 will help to increase the connectivity of all available data. As a result, the user experience will develop at another level of connectivity that uses all available information. Web 3.0 can also be called the web of everything and everywhere, because most of the things around you are connected to the Internet called the Internet of Things. In any case, we are slowly or surely reaching a level where all the things we use will certainly be available online and connected via the Internet. This idea has been around for decades, it has been in the works for a long time in a way and is called the Internet of Things.

IOT & USE CASES

Since there is still no unambiguous definition of the term Web 3.0, we are simultaneously moving alongside its development and beyond its framework towards the Internet of Things. IoT is likely to be the next stage of network development because it seems that one of the

*Corresponding author: branislav.sancanin@famns.edu.rs

features of the web we are heading towards and that is ubiquity, Brings IoT to a whole new level. Smart devices in the Internet of Things not only use the Internet, but also communicate with each other through machine-to-machine (M2M) communication to accomplish tasks without the need for people to interfere. Today, there are already many smart devices as well as fully automated internet-connected systems that work without human interference. The Internet is an extension of the network to the physical devices that we use every day. Embedded in the electronics of objects and things, with internet connectivity and the existence of certain sensors these devices can communicate with each other and transmit information to others via the Internet, and can be monitored and controlled remotely. The definition of IoT has evolved due to the synthesis of multiple different technologies, real-time analytics, machine learning, sensor development and embedded systems. The advancement of technologies in the field of development of wireless sensors, control systems, automation, integration of artificial neural networks has greatly contributed to the development of IoT. For the consumer market and most people, IoT technology is synonymous with products related to the concept of smart homes, which includes devices such as lighting, thermostats, home security systems and cameras and other small household appliances that support one or more common ecosystems and can be controlled via devices connected to that ecosystem, such as smartphones or smart speakers. The most significant trend in the Field of IoT is the explosive growth of internet-connected devices that can be controlled via the Internet. A very wide range of device management applications means that there are many ways in which certain devices can be controlled but a number of common features are slowly becoming standardized, further facilitating the expansion of IoT. Also, IoT creates opportunities for more direct integration of the physical world into computer systems, resulting in improved efficiency, economic growth and reduced human effort.

Since IoT is most often associated with smart homes, in terms of application it certainly finds its use there. Smart home IoT uses devices that connect a variety of sensors and combine the characteristics of multiple devices that are connected via IoT to make them available for remote monitoring, control, access, or to provide information and services that meet the needs of users. The first modern products for smart homes became available to consumers in the early 2000s. Smart home technology allows users to control and monitor their devices using apps on computers or phones as well as on any device that is connected. Users can remotely control all connected devices whether they are in or out of the house. This allows for far more efficient energy consumption as well as securing facilities. The technology used individually in homes is now used to make smart cities that function in a similar way to smart homes with the idea of monitoring everything much more efficiently and to save energy and reduce maintenance costs. One of the key features of smart home deployment is providing assistance to people with disabilities and the elderly. These systems use assistive technologies that adapt to the specific disability of the owner. Voice control helps people with limited vision and mobility while warning systems can be connected directly to appliances used by people with hearing impairments. Also, these characteristics can additionally include sensors that track medical emergencies such as attacks or falls. Smart home technology applied in this way gives its users more freedom and raises the quality of life.

The Internet of Medical Things is the application of IoT for medical and health purposes, data collection and analysis. Smart healthcare, as it is called, has led to the creation of a digitized health care system by linking available medical resources and health services. IoT devices can be used for the purpose of remote monitoring of the patient's health and a system that notifies health services in case of danger to the patient. Devices that allow health monitoring can be simple from monitors that monitor the heart, to devices that monitor specially installed implants such as pacemakers or advanced hearing aids. Some hospitals have even begun implementing the idea of "smart beds" that inform them in case patients try to get up without permission, and are also used for the purpose of adjusting beds in a certain way without physical interaction from medical personnel. As of 2018, the Internet of Medical Things has not only been applied in clinical trials but also in the wider health and health insurance industry. The IoT now allows doctors, patients and other individuals with access to be part of a system where patient records are stored in a database with constant access to the necessary patient information. Internet of Things systems are patient-centered. This also includes some flexibility in relation to current health conditions. IoT has also found application in health insurance - with the help of solutions based on bio-sensors and smart clothing that monitor user behavior, it is possible to process data more accurately and develop new pricing models for health insurance and services individually

and personalized for each user.

IoT can help integrate communication, control and information processing among different transport systems. Dynamic interaction among components of the transport system enables internal and external communication, smart traffic control, smart parking, electronic toll collection system, logistics, fleet management, vehicle correctness control, vehicle safety and roadside assistance. Sensors such as GPS sensors, air humidity and temperature sensors send data to the IoT platform then the data is analyzed and sent back to users. This way, users can monitor the condition of the vehicle in real time and make appropriate decisions. If this information is combined with machine learning, over time it can lead to and help reduce the number of traffic accidents in a number of ways, such as introducing warnings about sleepy drivers, critical road sections and possibly providing enough information for vehicles that will be autonomous on the roads.

IoT devices can be used to monitor and control mechanical, electrical and electronic systems used in various types of buildings e.g., public and private, industrial, institutions or residential, as well as in home automation and building automation systems. In this context, three main areas are dealt with in the literature:

• Integrating the Internet with energy management systems in buildings to create "smart buildings" energy efficient and managed via the Internet of Things,

• Possible real-time tracking methods to reduce energy consumption and track passenger behavior

• Integration of smart devices in the built environment and how they can know how they can be used autonomously in future applications

Monitoring and controlling the operations of urban and rural infrastructure such as bridges, railways and wind farms are one of the key applications of the Internet of Things. IoT infrastructure can be used to monitor all events or changes in structural conditions of infrastructure that may endanger safety and increase the risk of possible injuries and the like. IoT can benefit the construction industry by saving costs, reducing time, better quality workdays, paperless workflow and increasing productivity.[4] This can help make faster decisions and save money using real-time data analytics. It can also be used to plan repair and maintenance activities in an efficient way, by coordinating tasks between the various service providers and users of these facilities. IoT devices can also be used to control critical infrastructure such as bridges to provide access to ships. The use of IoT devices for monitoring and operational infrastructure is likely to improve incident management and emergency response coordination, as well as the quality of service, and thus reduce labor costs in all infrastructure areas. Even areas such as waste management can benefit from the automation and optimization brought about by the Internet of Things.

IoT can achieve seamless integration of various production machines equipped with sensor, identification, process, communication, driving and network capabilities. Based on such a highly integrated smart cyber physical space, it opens the door to creating new business and market opportunities for production. Network control and management of production equipment, asset management and production process situation or control bring IoT into the domain of industrial applications and smart manufacturing. Intelligent IoT systems enable fast production of new products, dynamic response to product requirements and optimization of production in real time as well as networks of supplier chains, by networking production machines, sensors and control systems together.

In agriculture, there are numerous Applications of IoT such as collecting data on temperature, precipitation, humidity, wind speed, pest infection, and soil content. This data can be used to automate agricultural techniques as well as make informed decisions to improve quality and quantity, minimize risks and waste, as well as reduce crop management efforts. For example, farmers can now monitor soil temperature and moisture from afar, and even apply internet of things data to precise fertilization programs that will help them improve production.

A significant number of power-consuming devices such as switches, sockets, light bulbs and TVs already have integrated internet connectivity. These devices allow remote user control or central control via a cloud-based interface, and enable functions such as planning e.g., remote power or turning off heating or cooling systems, stove control, changing lighting conditions, etc. This is only part of the ideas of using and applying use for IoT, in fact, IoT provides almost endless possibilities for connecting devices and equipment. In terms of creativity, this field is

wide open with an unlimited number of ways to network devices. IoT in addition to possibility carries with it potential security problems. Related to the privacy and security of the Internet of Things. [1]

IOT SECURITY AND MAIN PRIVACY ISSUES

As sensors and cameras become more common in everyday use, especially in public spaces, people have less and less knowledge of the information collected from them and have no way to avoid it. The potential that IoT has to invade privacy and cause security issues is worrying. Among the proposed solutions in terms of techniques that have applied and met the basic principles of privacy, only a few have shown satisfactory results. Despite the high security profiles and alarming flaws, device manufacturers remain indifferent. They focus on profitability, but not on safety. Consumers must have full control over the data collected, including the option to delete it if they choose to. Without ensuring privacy, spending in the "broad masses" simply won't happen.

Many people are embarrassed that companies collect information about them, and they are even more embarrassed to sell this information to everyone. The user is forced to give up all privacy (often in conditions such intricate and long texts that no one bothers to open them) or the client simply cannot access the service unless he agrees. This has led to ongoing discussions about consumer privacy and how best to educate consumers about privacy and data availability.

Security is the biggest concern in adopting Internet of Things technology. In particular, as IoT spreads rapidly, cyberattacks are likely to become more and more physical and less of a virtual threat. The current IoT comes with a number of security flaws. These weaknesses include poor authentication (IoT devices are used with default credentials), unencrypted messages sent between devices, SQL injections, and a lack of verification or encryption of software improvements. This allows attackers to easily intercept data to collect personally identifiable information, steal user credentials when logging in, or incorporate malware into a newly updated firmware. It's not a bad idea to wonder if IoT flaws will allow hackers to do whatever they want through interconnected devices and the vague and open question of who guarantees privacy and how to install security measures in new internet-connected devices. Mobile car owners can share the key remotely via the mobile app. In other words, it means nothing else that these same cars can be hijacked and stolen via their internet connections. Nevertheless, IoT enters its adolescence, as connected devices become smarter, more comprehensive and ubiquitous. Algorithms and data visualization schemes are also evolving. It is possible to test previous security flaws and previous cases of privacy breaches, thus providing more than necessary security for further widespread use of IoT in all areas. Security and risk management should not be taken lightly into account when creating new ways of using IoT, as new technologies come with new creative ways of misuse them.

MQTT STANDARDIZATION OF IOT – POTENTIAL SOLUTION

The suitability for reliable and efficient communication, even via unstable mobile networks and the networking of many thousands of devices, is required in many situations. This is why Message Queue Telemetry Transport (MQTT) is now one of the most important protocols in the Internet of Things. Since MQTT is mostly used in "machine to machine" and "Internet of Things" field, it is somewhat surprising that the history of the protocol begins as early as 1999. Since the mobile infrastructure at that time was disproportionate to the current expansion, there were significant challenges. One of them was data transmission via satellite and terrestrial networks with the lowest possible costs. A generic solution should also be found that goes beyond a direct point-to-point connection and decouples the sensors as data producers from the data users. [2]

PROTOCOL GOALS

To overcome the challenges, the following properties were developed for the protocol:

• The implementation must be simple in order to connect devices with limited resources.

• There must be different service qualities for data transmission so that transmission is also guaranteed in unstable networks.

• The transmission must simply and efficiently use the available bandwidth.

• Since meta information is often sent again when interrupted connections are resumed, it would be advantageous to store this on the server side (session awareness).

• The protocol should be able to transfer different data types and not be restricted to a specific structure (data-agnostic).

To achieve these goals, MQTT protocol was developed. In 2010, it was then officially released under open-source license and was brought as MQTT library under the umbrella of the Eclipse Foundation, further boosting the widespread use of the protocol. The goals identified technology for scalable real-time communication with minimal use of broadband and resources. Real-time means data transmission without polling or similar mechanisms. MQTT implements the publish/subscribe pattern. The paradigm shift from a request/response to an event-driven publish/subscribe architecture is the central aspect here. It replaces the point-to-point connections with a central server (broker) to which both data producers and users can connect. The sending (publishing) and receiving (subscribing) of messages works via so-called topics. A topic is a string that represents a kind of subject of the message, but is structured similarly to a URL. For example, a temperature sensor in a living room might post its current temperature on the following topic: Office/Hall/Temperature.

QUALITY CONTROL MECHANISMS

Another important concept is the three is the quality of service for data transmission 0, 1 and 2. MQTT is based on TCP, which is why both transmissions are very reliable. Nevertheless, this is not a sufficient solution for networks with many transmission errors due to connection problems, such as in mobile networks. Therefore, the protocol has built-in mechanisms that guarantee the successful transmission of messages. The assurance varies from no guarantee (level 0) to that the message will arrive at least once (level 1) to a guarantee that the message will arrive exactly once (level 2). The difference between level 1 and 2 is that at level 1 it can happen that a message reaches a client more often. Depending on the application, the appropriate level should be selected, because the higher the level, the higher the bandwidth required. [3]

LAST WILL AND RETAINED MESSAGES

Many problems can be solved with the possibilities of publish/subscribe and the use of QoS levels (Quality of Service). Since various clients lose the connection from time to time, it can happen that a mobile application that has reconnected does not know whether a temperature sensor is connected at all and what the current value of the sensor is. In addition, one does not know whether a sensor has failed. MQTT has the concepts “Last Will and Testament” and “Retained Messages” for these problems. When connecting, each client can send a message with its will to the broker, consisting of a topic and a message. As soon as the broker notices that the connection has been broken, it sends the message on behalf of the client. This only works if the application is connected at the time the sensor disconnects. A “retained message” can help here. It is a message stored by the broker and delivered to each client that reconnects and subscribes to the topic. Only one message can be saved for each topic. This can be used to store, for example, the last value of the sensor on the topic Home/Living Room/Temperature or the status of the sensor on Home/Living Room/Temperature/Status. This means that newly connected devices can also receive the last value, even if they were not connected at the time of sending. [5]

RECORD SECURITY

Due to the publish-subscribe architecture, MQTT has hardly any attack vectors when sending data to a specific client, since clients always initiate the TCP connection to the broker themselves and it is not possible to open the connections from the outside. This means that there are no risks when using network address translation (NAT), as is often the case in local

networks, for example. Devices don't have to (and shouldn't) be addressable via the Internet. Brute force and denial of service attacks on individual devices are difficult to carry out because the devices cannot be addressed from the outside. MQTT should always be used in conjunction with TLS so that all communication is encrypted. This makes it possible to largely avoid man-in-the-middle attacks, i.e., attacks in which a middleman can read or even manipulate data. To do this, the MQTT client must check the server certificate and ensure that it matches the desired MQTT broker and is trustworthy. The mechanism is the same as with HTTPS. When initially establishing a connection to an MQTT broker, a client can optionally use both a user name and a password for authentication. These two parameters are the basis for a simple credential-based authentication, but also for more complex authentication methods like OAuth 2.0. Depending on the range of functions of the MQTT broker, different authentication methods can be used.

CLEAN LOGIN

Authentication refers to checking the access data provided by the client at the broker. This makes it possible to determine whether the MQTT client is actually who it claims to be. For example, if a password does not match the specified username, the broker rejects the connection. MQTT sessions always begin with a client establishing a connection and the associated initial MQTT CONNECT packet. In addition to properties such as the unique client identifier, it can optionally contain a user name and password. In the simplest case, the client sends a user name and the associated password in plain text. In the best case, the broker does not have the password in plain text, but only the cryptographic hash of the password - SHA-512 is a suitable algorithm. This allows the broker to calculate the hash of the password transmitted in plain text itself and compare it with the known credentials. Of course, it is even better if the MQTT client only transmits its password as a hash and the MQTT broker never comes into contact with the original password in plain text. A basic principle for IoT devices should be that each gets individual access data so that administrators can block individual accesses if necessary. In professional MQTT installations, the credentials are usually managed centrally. Therefore, the MQTT broker often requires integration with external systems such as databases, LDAP directories or microservices. Professional brokers usually offer a plug-in system that allows integration with little effort. [3]

MQTT AUTHOTIZATION

In addition to authentication, authorization is an important concept for securing MQTT. Authorization refers to the granting of special rights and clarifies the question of what a specific client is allowed to do. Successful authentication of an MQTT client does not necessarily mean that it has permission to perform all actions. In concrete terms, MQTT developers usually restrict which topics a client can send messages for and which topics they can subscribe to. Without this authorization, a malicious client could subscribe to messages from all topics and thus read data that is not intended for it without authorization. In addition, such a client could itself send messages with any topic. Therefore, a clean application with MQTT absolutely includes protection with authorization mechanisms. MQTT brokers for business-critical use usually offer fine-grained authorization mechanisms. In addition, users should configure restrictions for each MQTT client, such as the maximum message size that a client is allowed to send and the maximum bandwidth for an MQTT sender. This ensures that no individual MQTT clients attempt to carry out denial-of-service attacks on the broker through software errors or malicious intent and, if successful, endanger the entire MQTT service.

CONCLUSION

Despite the delays in the standard, MQTT is an open and productive protocol whose main applications are in the area of the Internet of Things. The scaling to many thousands of simultaneously connected devices and the efficiencies in transmission and resource utilization of the devices provide a solution to problems that legacy HTTP cannot address. The display and alerting of live data from sensors on mobile devices and web browsers offer developers the

opportunity to increase the added value of their applications. The user thus has more up-to-date data and there are fewer costs on both sides. The company develops scalable communication solutions and web dashboards based on MQTT as building blocks for applications in the area of the Internet of Things and Industry 4.0. There are some basic security mechanisms that should be self-evident in every MQTT installation. This includes the fact that MQTT should never be used over the Internet without transport encryption via TLS - just as it has now become an anti-pattern to transmit unencrypted data on the World Wide Web via HTTP. Developers should definitely implement an authentication and an authorization strategy so that MQTT clients can receive fine-grained permissions and only trustworthy clients are allowed to communicate with the MQTT broker. MQTT can be used extremely flexibly. In order to make the use of MQTT secure over the Internet or locally, the protocol, like the Internet protocols HTTP or FTP, relies on underlying security protocols such as TLS. In addition to authentication via username and password, other measures such as using X.509 client certificates or OAuth 2.0 can be combined very well with MQTT. The additional use of user data encryption helps for critical and important messages. Basically, MQTT that uses measures presented in this paper can be operated quite easily and securely.

REFERENCES

[1] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), 2015, pp. 336-341, doi: 10.1109/ICITST.2015.7412116.

[2] W. T. Su, W. C. Chen and C. C. Chen, "An Extensible and Transparent Thing-to-Thing Security Enhancement for MQTT Protocol in IoT Environment," 2019 Global IoT Summit (GIoTS), 2019, pp. 1-4, doi: 10.1109/GIOTS.2019.8766412.

[3] F. Hmissi and S. Ouni, "TD-MQTT: Transparent Distributed MQTT Brokers for Horizontal IoT Applications," 2022 IEEE 9th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2022, pp. 479-486, doi: 10.1109/SETIT54465.2022.9875881.

C. S. Park and H. M. Nam, "Security Architecture and Protocols for Secure MQTT-SN," in IEEE Access, vol. 8, pp. 226422-226436, 2020, doi: 10.1109/ACCESS.2020.3045441.

4] T. K. Boppana and P. Bagade, "Security risks in MQTT-based Industrial IoT Applications," 2022 IEEE International Conference on Omni-layer Intelligent Systems (COINS), 2022, pp. 1-5, doi: 10.1109/COINS54846.2022.9854993.

[5] O. Sadio, I. Ngom and C. Lishou, "Lightweight Security Scheme for MQTT/MQTT-SN Protocol," 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), 2019, pp. 119-123, doi: 10.1109/IOTSMS48152.2019.8939177.